VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

a IPB

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

EPPING HERMANN & FISCHER
Ridlerstrasse 55
80339 München
ALLEMAGNE

EINGANG
Epping Hermann & Fischer
20. Aug. 2003
Frist: 07/09/2003

IPER: 18.10.2003
and. ba

PCT

SCHRIFTLICHER BESCHEID
(Regel 66 PCT)

Pages: 9
Sent by fax in advance

Absendedatum *(Tag/Monat/Jahr)*	18.08.2003
Aktenzeichen des Anmelders oder Anwalts: P2001,0154WO N	**ANTWORT FÄLLIG** innerhalb von **0 Monat(en) und 20Tagen** ab obigem Absendedatum

Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/DE02/00616	20/02/2002	12/03/2001

Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK
G06F1/00

Anmelder
INFINEON TECHNOLOGIES AG et al.

1. Dieser Bescheid ist der **erste** schriftliche Bescheid der mit der internationalen vorläufigen Prüfung beauftragte Behörde

2. Dieser Bescheid enthält Angaben zu folgenden Punkten:

I	☒	Grundlage des Bescheides
II	☐	Priorität
III	☐	Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
IV	☐	Mangelnde Einheitlichkeit der Erfindung
V	☒	Begründete Feststellung nach Regel 66.2(a)(ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
VI	☐	Bestimmte angeführte Unterlagen
VII	☐	Bestimmte Mängel der internationalen Anmeldung
VIII	☐	Bestimmte Bemerkungen zur internationalen Anmeldung

3. Der Anmelder wird **aufgefordert**, zu diesem Bescheid **Stellung zu nehmen**

Wann? Siehe oben genannte Frist. Der Anmelder kann vor Ablauf dieser Frist bei der Behörde eine Verlängerung beantragen, siehe Regel 66.2 d).

Wie? Durch Einreichung einer schriftlichen Stellungnahme und gegebenenfalls von Änderungen nach Regel 66.3. Zu Form und Sprache der Änderungen, siehe Regeln 66.8 und 66.9.

Dazu: Hinsichtlich einer zusätzlichen Möglichkeit zur Einreichung von Änderungen, siehe Regel 66.4.
Hinsichtlich der Verpflichtung des Prüfers, Änderungen und/oder Gegenvorstellungen zu berücksichtigen, siehe Regel 66.4 bis.
Hinsichtlich einer formlosen Eröterung mit dem Prüfer, siehe Regel 66.6.

Wird keine Stellungnahme eingereicht, so wird der internationale vorläufige Prüfungsbericht auf der Grundlage dieses Bescheides erstellt.

4. Der Tag, an dem der internationale vorläufige Prüfungsbericht gemäß Regel 69.2 spätestens erstellt sein muß, ist der: 12/07/2003.

Name und Postanschrifft der mit der internationalen Prüfung beauftragte Behörde:
Europäisches Patentamt - Gitschiner Str. 103
D-10958 Berlin
Tel. +49 30 25901 - 0
Fax: +49 30 25901 - 840

Bevollmächtigter Bediensteter / Prüfer
Carnerero Álvaro, F

Formalsachbearbeiter (einschl. Fristverlängerung)
Tsogka, P
Tel. +49 30 25901 727

I. Grundlage des Bescheids

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Bescheids als "ursprünglich eingereicht"*):

Beschreibung, Seiten:

1-15 ursprüngliche Fassung

Patentansprüche, Nr.:

1-16 ursprüngliche Fassung

Zeichnungen, Blätter:

1 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Regel 66.2(a)(ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ansprüche	
Erfinderische Tätigkeit (IS)	Ansprüche	1-16
Gewerbliche Anwendbarkeit (IA)	Ansprüche	

2. Unterlagen und Erklärungen:
   siehe Beiblatt

1.1 Es wird auf das folgende Dokument verwiesen:

D1: MENEZES A J ET AL: 'Handbook of Applied Cryptography, passage' HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICS AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, Seiten 294-296, 400-401, 506-508, 512-515 XP002219455 ISBN: 0-8493-8523-7

1.2 Die Seiten 512 bis 515 von D1 wurden im internationalen Recherchenbericht nicht angegeben. Eine Kopie dieser zusätzlichen Seiten liegt bei.

2. Die vorliegende Anmeldung erfüllt nicht die in Artikel 33 PCT genannten Kriterien, weil der Gegenstand der Ansprüche 1 bis 16 nicht erfinderisch im Sinne von Artikel 33(3) PCT ist.

2.1 Dokument D1, das als nächstliegender Stand der Technik angesehen wird, offenbart ein Protokoll zum symmetrischen Schlüsselaustausch zwischen zwei Einheiten, bei dem die erste Einheit über einen öffentlichen und einen privaten Schlüssel verfügt und auf eine dem ElGamal-Algorithmus ähnliche Verschlüsselungsmethode zurückgreift, umfassend die Schritte:

a) die zweite Einheit verschlüsselt den gemeinsamen symmetrischen Schlüssel mittels des der zweiten Einheit bekannten öffentlichen Schlüssels der ersten Einheit und übermittelt den verschlüsselten symmetrischen Schlüssel an die erste Einheit;

b) Die erste Einheit entschlüsselt den gemeinsamen symmetrischen Schlüssel mittels des nur ihr bekannten privaten Schlüssels.

2.2 Dokument D1 offenbart auch ein herkömmliches symmetrisches Challenge-Response-Protokoll. Dabei handelt es sich um ein Verfahren zur Authentikation einer ersten beweisführenden Einheit gegenüber einer zweiten verifizierenden Einheit, bei dem sowohl die beweisführende Einheit als auch die verifizierende Einheit einen gemeinsamen symmetrischen Schlüssel kennen. Die beweisführende Einheit stellt ihre Kenntnis des gemeinsamen symmetrischen

Schlüssels unter Beweis durch die Verschlüsselung eines im voraus an die verifizierende Einheit unverschlüsselt übermittelten Datenelements mittels des besagten gemeinsamen Schlüssels.

2.3 Es liegt nahe, das zweite Verfahren zu verwenden nachdem das erste Protokoll beendet ist. Auf diese Weise stellt die beweisführende Einheit die Kenntnis ihres asymmetrischen privaten Schlüssels anhand eines symmetrischen Challenge-Response-Protokolls unter Beweis. Solche hybriden Verfahren sind etwa aus dem Beller-Yacobi-Protokoll zum Schlüsselaustausch bekannt (siehe Seiten 512-515 vom zitierten Dokument).

Der Gegenstand der Ansprüche beruht somit nicht auf einer erfinderischen Tätigkeit und erfüllt damit nicht das in Artikel 33(3) PCT genannte Kriterium.